United States Government Accountability Office

GAO

Report to the Commissioner of Internal Revenue

January 2009

INFORMATION SECURITY

Continued Efforts Needed to Address Significant Weaknesses at IRS

GAO

Accountability * Integrity * Reliability

GAO-09-136

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-09-136, a report to the Commissioner of Internal Revenue

Why GAO Did This Study

The Internal Revenue Service (IRS) relies extensively on computerized systems to carry out its demanding responsibilities to collect taxes (about $2.7 trillion in fiscal years 2008 and 2007), process tax returns, and enforce the nation's tax laws. Effective information security controls are essential to protect financial and taxpayer information from inadvertent or deliberate misuse, improper disclosure, or destruction.

As part of its audits of IRS's fiscal years 2008 and 2007 financial statements, GAO assessed (1) the status of IRS's actions to correct previously reported weaknesses and (2) whether controls were effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer information. To do this, GAO examined IRS information security policies and procedures and other documents; tested controls over key financial applications; and interviewed key agency officials.

What GAO Recommends

To fully implement an agencywide information security program, GAO recommends that the Commissioner of Internal Revenue (1) ensure risk assessments for IRS systems are reviewed at least annually and (2) implement steps to improve the testing and evaluating of controls. In commenting on a draft of this report, IRS agreed to develop a plan addressing each of the recommendations.

To view the full product, including the scope and methodology, click on GAO-09-136. For more information, contact Nancy Kingsbury at (202) 512-2700 or kingsburyn@gao.gov or Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

January 2009

INFORMATION SECURITY

Continued Efforts Needed to Address Significant Weaknesses at IRS

What GAO Found

IRS has continued to make progress in correcting previously reported information security weaknesses. It has corrected or mitigated 49 of the 115 weaknesses that GAO reported as unresolved during its last audit. For example, the agency

- implemented controls for unauthenticated network access and user IDs on the mainframe,
- encrypted sensitive data going across its network,
- improved the patching of critical vulnerabilities, and
- updated contingency plans to document critical business processes.

However, most of the previously identified weaknesses remain unresolved. For example, IRS continues to, among other things, allow sensitive information, including IDs and passwords for mission-critical applications, to be readily available to any user on its internal network, and grant excessive access to individuals who do not need it. According to IRS officials, they are continuing to address the uncorrected weaknesses and, subsequent to GAO site visits, had completed additional corrective actions.

Despite IRS's progress, information security control weaknesses continue to jeopardize the confidentiality, integrity, and availability of financial and sensitive taxpayer information. IRS did not consistently implement controls that were intended to prevent, limit, and detect unauthorized access to its systems and information. For example, IRS did not always

- enforce strong password management for properly identifying and authenticating users;
- authorize user access, including access to personally identifiable information, to permit only the access needed to perform job functions;
- encrypt certain sensitive data;
- effectively monitor changes on its mainframe; and
- physically protect its computer resources.

A key reason for these weaknesses is that IRS has not yet fully implemented its agencywide information security program to ensure that controls are appropriately designed and operating effectively. Specifically, IRS did not annually review risk assessments for certain systems, comprehensively test for certain controls, or always validate the effectiveness of remedial actions. Until these weaknesses are corrected, the agency remains particularly vulnerable to insider threats and IRS is at increased risk of unauthorized access to and disclosure, modification, or destruction of financial and taxpayer information, as well as inadvertent or deliberate disruption of system operations and services.

Contents

Abbreviations

CIO	Chief Information Officer
FISMA	Federal Information Security Management Act
IG	Inspector(s) General
MITS	Modernization and Information Technology Services
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget

GAO

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

January 9, 2009

The Honorable Douglas Shulman
Commissioner of Internal Revenue

Dear Commissioner Shulman:

The Internal Revenue Service (IRS) has a demanding responsibility in collecting taxes, processing tax returns, and enforcing the nation's tax laws. It relies extensively on computerized systems to support its financial and mission-related operations. Effective information system controls are essential for protecting the confidentiality, integrity, and availability of financial and sensitive taxpayer information and ensuring that information is adequately protected from inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction.

As part of our audit of IRS's fiscal years 2008 and 2007 financial statements,[1] we assessed the effectiveness of the agency's information security controls[2] over key financial systems, information, and interconnected networks at four locations. These systems support the processing, storage, and transmission of financial and sensitive taxpayer information. In our report on IRS's fiscal years 2008 and 2007 financial statements, we reported that the new information security deficiencies we identified in fiscal year 2008 and the unresolved deficiencies from prior audits represent a material weakness[3] in internal controls over financial and tax processing systems.

[1] GAO, *Financial Audit: IRS's Fiscal Years 2008 and 2007 Financial Statements*, GAO-09-119 (Washington, D.C.: Nov. 10, 2008).

[2] Information security controls include logical and physical access controls, configuration management, segregation of duties, and continuity of operations. These controls are designed to ensure that access to data is appropriately restricted, that physical access to sensitive computing resources and facilities is protected, that only authorized changes to computer programs are made, that incompatible duties are segregated among individuals, and that back-up and recovery plans are adequate to ensure the continuity of essential operations.

[3] A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected.

We assessed (1) the status of IRS's actions to correct or mitigate previously reported information security weaknesses and (2) whether controls over key financial and tax processing systems are effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer information. We conducted this work from April 2008 to January 2009, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. For additional information about our objectives, scope, and methodology, refer to appendix I.

Results in Brief

IRS has continued to make progress in correcting previously reported information security weaknesses. It has corrected or mitigated 49 of the 115 information security weaknesses that we reported as unresolved at the time of our last review. For example, the agency implemented controls for unauthenticated network access and user IDs on the mainframe, encrypted sensitive data going across its network, improved the patching of critical vulnerabilities, and updated contingency plans to document critical business processes. In addition, IRS has several initiatives under way that are designed to improve information security, such as implementing a comprehensive plan to address numerous weaknesses related to network and system access, among other issues. However, about 57 percent of the previously identified weaknesses remain unresolved. For example, IRS continues to, among other things, allow sensitive information, including IDs and passwords for mission-critical applications, to be readily available to any user on its internal network, and grant excessive access to individuals who do not need it. According to IRS officials, they are continuing to address the uncorrected weaknesses and, subsequent to our site visits, had completed additional corrective actions.

Despite IRS's progress, information security control weaknesses continue to jeopardize the confidentiality, integrity, and availability of financial and sensitive taxpayer information. IRS did not consistently implement controls that were intended to prevent, limit, and detect unauthorized access to its systems and information. For example, IRS did not always (1) enforce strong password management for properly identifying and authenticating users; (2) authorize user access, including access to personally identifiable information, to permit only the access needed to perform job functions; (3) encrypt certain sensitive data; (4) effectively monitor changes on its mainframe; and (5) physically protect its computer resources. A key reason for these weaknesses is that IRS has not yet fully implemented its agencywide information security program to ensure that controls are appropriately designed and operating effectively. Specifically, IRS did not review risk assessments at least annually for certain systems, comprehensively test certain controls, or always validate the effectiveness of remedial actions. Until these weaknesses are corrected, the agency remains particularly vulnerable to insider threats and IRS is at increased risk of unauthorized access to and disclosure, modification, or destruction of financial and taxpayer information, as well as inadvertent or deliberate disruption of system operations and services.

We are making recommendations to the Commissioner of Internal Revenue to fully implement a comprehensive agencywide information security program. In a separate report with limited distribution, we are making recommendations to correct the specific weaknesses we identified during our review.

In providing written comments on a draft of this report, the Commissioner of Internal Revenue stated that the security and privacy of taxpayer information is of the utmost importance to the agency and noted that IRS is committed to securing its computer environment as it continually evaluates processes, promotes user awareness, and applies innovative ideas to increase compliance. He further stated that IRS would develop a detailed corrective action plan addressing each of our recommendations.

Background

Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where maintaining the public's trust is essential. The dramatic expansion in computer interconnectivity and the rapid increase in the use of the Internet have revolutionized the way our government, our nation, and much of the world communicates and conducts business. Although this expansion has created many benefits for agencies such as IRS in achieving their missions and providing information to the public, it also exposes federal networks and systems to various threats.

Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intent who can intrude and use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other computer systems and networks. The risks to these systems are well-founded for a number of reasons, including the dramatic increase in reports of security incidents, the ease of obtaining and using hacking tools, and steady advances in the sophistication and effectiveness of attack technology. For example, the Office of Management and Budget cited[4] a total of 12,198 incidents reported to the U.S. Computer Emergency Readiness Team (US-CERT)[5] by federal agencies during fiscal year 2007, which is more than twice the number of incidents reported the prior year. The Federal Bureau of Investigation has identified multiple sources of threats, including foreign nation states engaged in intelligence gathering and information warfare, domestic criminals, hackers, virus writers, and disgruntled employees or contractors working within an organization. In addition, the U.S. Secret Service and the CERT Coordination Center[6] studied insider threats and stated in a May 2005 report that "insiders pose a substantial threat by virtue of their knowledge of, and access to, employer systems and/or databases."

Our previous reports, and those by federal inspectors general, describe persistent information security weaknesses that place federal agencies, including IRS, at risk of disruption, fraud, or inappropriate disclosure of sensitive information. Accordingly, we have designated information security as a governmentwide high-risk area since 1997,[7] a designation that remains in force today.

Recognizing the importance of securing federal agencies' information systems, Congress enacted the Federal Information Security Management Act (FISMA) in December 2002[8] to strengthen the security of information and systems within federal agencies. FISMA requires each agency to

[4] OMB, *Fiscal Year 2007 Report to Congress on Implementation of the Federal Information Security Management Act of 2002* (Washington, D.C.: March 2008).

[5] US-CERT's mission is to protect the nation's Internet infrastructure. US-CERT coordinates defense against and responses to cyber attacks by analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.

[6] The CERT Coordination Center is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

[7] GAO, *High-Risk Series: Information Management and Technology*, GAO/HR-97-9 (Washington, D.C.: February 1997).

[8] FISMA was enacted as title III, E-Government Act of 2002, Pub L. No. 107-347, Dec. 17, 2002.

develop, document, and implement an agencywide information security program for the information and systems that support the operations and assets of the agency, using a risk-based approach to information security management. Such a program includes assessing risk; developing and implementing cost-effective security plans, policies, and procedures; providing specialized training; testing and evaluating the effectiveness of controls; planning, implementing, evaluating, and documenting remedial actions to address information security deficiencies; and ensuring continuity of operations.

IRS has demanding responsibilities in collecting taxes, processing tax returns, and enforcing the nation's tax laws, and relies extensively on computerized systems to support its financial and mission-related operations. IRS collected about $2.7 trillion in tax payments in fiscal years 2008 and 2007; processed hundreds of millions of tax and information returns; and paid about $426 billion and $292 billion, respectively, in refunds to taxpayers. Further, the size and complexity of IRS adds unique operational challenges. The agency employs tens of thousands of people in its Washington, D.C., headquarters, 10 service center campuses, 3 computing centers, and numerous other field offices throughout the United States. IRS also collects and maintains a significant amount of personal and financial information on each American taxpayer. The confidentiality of this sensitive information must be protected; otherwise, taxpayers could be exposed to loss of privacy and to financial loss and damages resulting from identity theft or other financial crimes.

The Commissioner of Internal Revenue has overall responsibility for ensuring the confidentiality, integrity, and availability of the information and information systems that support the agency and its operations. FISMA requires the Chief Information Officers (CIO) at federal agencies to be responsible for developing and maintaining an information security program. Within IRS, this responsibility is delegated to the Associate CIO for Cybersecurity. The Office of Cybersecurity is within the CIO's Modernization and Information Technology Services (MITS) organization. The mission of MITS is to deliver information technology services and solutions that drive effective tax administration to ensure public confidence. MITS's goals are to improve service, deliver modernization, increase value, and assure the security and resilience of IRS information systems and data. The Office of Cybersecurity is responsible for ensuring IRS's compliance with federal laws, policies, and guidelines governing measures to assure the confidentiality, integrity, and availability of IRS electronic systems, services, and data. The Office of Cybersecurity is to manage IRS's information security program in accordance with FISMA, including to perform assessments of risks; track compliance; identify, mitigate and monitor cybersecurity threats; determine strategy and priorities; and monitor security program implementation. In order for IRS organizations to carry out their respective responsibilities in information security, information security policies, guidelines, standards and procedures have been developed and published in the *Internal Revenue Manual.*

IRS Demonstrated Progress in Correcting Previously Reported Weaknesses

Although IRS has continued to make progress toward correcting previously reported information security weaknesses at three data centers and an additional facility, many deficiencies remain. It has corrected or mitigated 49 of the 115 information security weaknesses that we reported as unresolved at the time of our last review. IRS corrected weaknesses related to access controls, including physical security, among others. For example, it has

- implemented controls for unauthenticated network access and user IDs on the mainframe;
- further limited access to its mainframe environment by limiting access to system management utility functions and mainframe console commands;
- taken several measures to protect information traversing its network, such as installing a secure communication service for encryption;
- taken steps to improve its auditing and monitoring capability by retaining audit logs of security-relevant events for its administrative accounting system and ensuring that audit logs were being created for such events on its procurement system;
- removed authority for unrestricted physical access to the computer room and tape library from individuals who did not need it to perform their job;
- improved controls over physical access proximity cards;
- enhanced periodic reviews of mainframe configurations;
- improved the disposal of removable media;

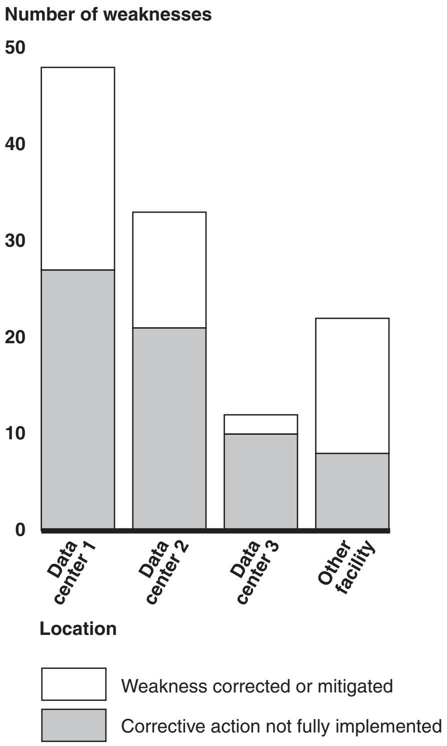
- improved patching of critical vulnerabilities, as well as the timeliness of applying patches at certain facilities; and

- updated contingency plans to document critical business processes.

In addition, IRS has made progress in improving its information security program. For example, the agency completed an organizational realignment, including creation of the Associate CIO for Cybersecurity position, and has several initiatives under way that are designed to improve information security. IRS has developed and documented a detailed road map to guide its efforts in targeting critical weaknesses. Additionally, it is in the process of implementing a comprehensive plan to address numerous information security weaknesses, such as those associated with network and system access, audit trails, system software configuration, security roles and responsibilities, and contingency planning. These efforts are a positive step toward improving the agency's overall information security posture.

Although IRS has moved to correct previously identified security weaknesses, 66 out of 115 weaknesses—or about 57 percent—remained open or unmitigated at the time of our site visits (see fig. 1).

Figure 1: Previously Identified Weaknesses at IRS Locations



Source: GAO analysis of agency data.

Unmitigated deficiencies include those related to access controls, as well as other controls such as configuration management and personnel security. For example, IRS continues to, among other things,

- allow sensitive information, including user IDs and passwords for mission-critical applications, to be readily available to any user on IRS's internal network;

- use passwords that are not complex enough to avoid being guessed or cracked;

- grant excessive electronic access to individuals;

- inconsistently apply patches; and

- not remove separated employees' access in a timely manner for one of its systems.

Such weaknesses increase the risk of compromise of critical IRS systems and information. According to IRS officials, they are continuing to address the uncorrected weaknesses, and subsequent to our site visits, they had completed corrective actions for some of the weaknesses.

Weaknesses Placed Financial and Taxpayer Information at Risk

Although IRS has continued to make progress toward correcting previously reported information security weaknesses at its three data centers, as well as an additional facility, many deficiencies remain. These deficiencies include those related to access controls, as well as other controls such as configuration management and personnel security. A key reason for these weaknesses is that IRS has not yet fully implemented its agencywide information security program to ensure that controls are appropriately designed and operating effectively. Furthermore, these weaknesses continue to jeopardize the confidentiality, integrity, and availability of IRS's systems and contributed to IRS's material weakness in information security during the fiscal year 2008 financial statement audit.

IRS Did Not Fully Implement Access Controls

A basic management objective for any organization is to protect the resources that support its critical operations from unauthorized access. Organizations accomplish this objective by designing and implementing controls that are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities. Inadequate access controls potentially diminish the reliability of computerized information and increase the risk of unauthorized disclosure, modification, and destruction of sensitive information and disruption of service. Access controls include those related to user identification and authentication, authorization, cryptography, audit and monitoring, and physical security. IRS did not fully implement controls in the areas listed above, as the following sections in this report demonstrate.

Weaknesses Exist in Controls for Identification and Authentication

A computer system must be able to identify and authenticate different users so that activities on the system can be linked to specific individuals. When an organization assigns unique user accounts to specific users, the system is able to distinguish one user from another—a process called identification. The system also must establish the validity of a user's claimed identity by requesting some kind of information, such as a password, that is known only by the user—a process known as authentication. The combination of identification and authentication—such as user account/password combinations—provides the basis for establishing individual accountability and for controlling access to the system. According to the *Internal Revenue Manual*, passwords should be protected from unauthorized disclosure and modification when stored and transmitted. The *Internal Revenue Manual* also requires IRS to enforce strong passwords for authentication (defined as a minimum of eight characters, containing at least one numeric or special character, and a mixture of at least one uppercase and one lowercase letter).

Although IRS had implemented controls for identification and authentication, weaknesses continued to exist at two of the sites we visited. Specifically, usernames and passwords were still viewable on an IRS contractor-maintained Web site at one of its data centers. In addition, the agency continued to store passwords in scripts and did not enforce the use of strong passwords for systems at another data center. As a result, increased risk exists that an individual could view or guess these passwords and use them to gain unauthorized access to IRS systems.

Users Have More System Access Than Needed to Perform Their Jobs

Authorization is the process of granting or denying access rights and permissions to a protected resource, such as a network, a system, an application, a function, or a file. A key component of granting or denying access rights is the concept of "least privilege." Least privilege is a basic principle for securing computer resources and information. This principle means that users are granted only those access rights and permissions that they need to perform their official duties. To restrict legitimate users' access to only those protected resources that they need to do their work, organizations establish access rights and permissions. "User rights" are allowable actions that can be assigned to individual users or groups of users. File and directory permissions are rules that regulate which users can access a particular file or directory and the extent of that access. To avoid unintentionally authorizing users' access to sensitive files and directories, an organization must give careful consideration to its assignment of rights and permissions. The *Internal Revenue Manual* requires that system access be assigned based on least privilege—allowing access at the minimum level necessary to support the user's job duties. The *Internal Revenue Manual* also specifies that only individuals having a "need to know" in the performance of their duties should have access to sensitive information including that deemed as personally identifiable information.

IRS permitted users more privileges on its systems than needed to perform their official duties. For example, IRS integrated network device controls with its Windows management controls that could provide users with excessive access to its network infrastructure. According to IRS officials, the agency made a cost-based decision to implement this configuration. In addition, IRS did not restrict access to sensitive personally identifiable information. To illustrate, the agency allowed authenticated users on its network access to shared drives containing taxpayer information, as well as performance appraisal information for IRS employees including their social security numbers. This information could allow someone to commit fraud or identity theft. In another example, the agency did not restrict access to tax data for a major corporation and allowed all employees with network access the potential to view this information. These excessive privileges could allow users unwarranted access to IRS's network or enable them to access information not needed for their jobs and could place IRS systems or information at risk.

IRS Transmitted Certain Sensitive Data Across Its Network Unencrypted

Cryptography underlies many of the mechanisms used to enforce the confidentiality and integrity of critical and sensitive information. A basic element of cryptography is encryption. Encryption can be used to provide basic data confidentiality and integrity by transforming plain text into cipher text using a special value known as a key and a mathematical process known as an algorithm. IRS policy requires the use of encryption for transferring sensitive but unclassified information between IRS facilities. The National Security Agency also recommends disabling protocols that do not encrypt information transmitted across the network, such as user ID and password combinations.

Although IRS had implemented controls to encrypt information traversing its network, it did not always ensure certain sensitive data was encrypted. For example, one data center has not yet disabled unencrypted protocol services for all its UNIX servers. Similarly, at another center, users' login information is still being sent across the IRS internal network in clear text, potentially exposing account usernames and passwords. More importantly, IRS continues to transmit data, such as account and financial information, from its financial accounting system using an unencrypted protocol. By transmitting data unencrypted, IRS is at increased risk that an unauthorized individual could view sensitive information.

IRS Did Not Always Effectively Monitor Its Systems

To establish individual accountability, monitor compliance with security policies, and investigate security violations, it is crucial to know what, when, and by whom specific actions have been taken on a system. Organizations accomplish this by implementing system or security software that provides an audit trail, or logs of system activity, that they can use to determine the source of a transaction or attempted transaction and to monitor users' activities. The way in which organizations configure system or security software determines the nature and extent of information that can be provided by the audit trail. To be effective, organizations should configure their software to collect and maintain audit trails that are sufficient to track security-relevant events.

IRS did not always effectively monitor its systems. For example, IRS had not configured security software controls to log changes to datasets that would support effective monitoring of the mainframe at one of its data centers. In addition, other weaknesses include inadequate logging of security-relevant events for UNIX and Windows servers at one data center and for UNIX servers at another. By not effectively logging changes to its systems, IRS will not have assurance that it will be able to detect unauthorized system changes that could adversely affect operations, or appropriately detect security-relevant events.

IRS Did Not Always Fully Implement Controls for Physical Security

Physical access controls are used to mitigate the risks to systems, buildings, and supporting infrastructure related to their physical environment and to control the entry and exit of personnel in buildings, as well as data centers containing agency resources. Examples of physical security controls include perimeter fencing, surveillance cameras, security guards, and locks. Without these protections, IRS computing facilities and resources could be exposed to espionage, sabotage, damage, and theft. The *Internal Revenue Manual* requires that all authorized visitors and their packages and briefcases be examined when entering an IRS facility. In addition, data center security checkpoint procedures require that officers specifically screen for cameras and other items that are prohibited from IRS facilities. The *Internal Revenue Manual* also states that the authorized access list into restricted areas will be prepared monthly and dated and signed by the branch chief, but not before the branch chief validates the need of individuals to access the restricted area.

Although IRS had implemented numerous physical security controls, certain controls were not working as intended, and the agency had not fully implemented others. For example, security guards at one data center did not ensure that visitors and their possessions were properly screened when entering the facility. Our staff inadvertently included digital cameras in packed luggage. Despite screening the luggage with the magnetometer, the guards did not confront them about the prohibited items. In another example, IRS prepared access lists identifying personnel authorized to enter sensitive areas at two centers and at an additional facility; however, the branch chiefs at the three sites had not signed or dated the lists as required. This step is essential in verifying that employees continue to warrant access into restricted areas. As a result, increased risk exists that prohibited items and individuals may inappropriately be permitted access to IRS facilities and restricted areas.

IRS Had Not Fully Implemented Other Information Security Controls

In addition to access controls, other important controls should be in place to ensure the confidentiality, integrity, and availability of an organization's information. These controls include policies, procedures, and techniques for securely configuring information systems and implementing personnel security. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of IRS's information and information systems.

Configuration Management Requirements Were Inconsistently Implemented

The purpose of configuration management is to establish and maintain the integrity of an organization's work products. The *Internal Revenue Manual* states that IRS shall establish and maintain baseline configurations and inventories of organizational information systems and monitor and control any changes to the baseline configurations. Proactively managing vulnerabilities of systems will reduce or eliminate the potential for exploitation and involves considerably less time and effort than responding after an exploit has occurred. Patch management, a component of configuration management, is an important factor in mitigating software vulnerability risks. Patch installation can help diminish vulnerabilities associated with flaws in software code. Attackers often exploit these flaws to read, modify, or delete sensitive information; disrupt operations; or launch attacks against other organizations' systems. The *Internal Revenue Manual* requires that all vendor-supplied security patches be installed on all IRS systems.

IRS did not fully implement its policies for managing changes to its systems. Specifically, IRS did not maintain or enforce a baseline configuration for one data center's mainframe system, which supports the revenue accounting system of record and other applications. In addition, IRS used an unsupported software package that was not current and thus vulnerable to attack. Specifically, certain IRS servers were running an outdated version of software that was no longer supported by the vendor and, therefore, could not be patched against a known vulnerability. As a result, IRS has limited assurance that system changes are being properly monitored and that its systems are protected against new vulnerabilities.

IRS Did Not Always Implement Personnel Security Controls

The greatest harm or disruption to a system comes from the actions, both intentional and unintentional, of individuals. These intentional and unintentional actions can be reduced through the implementation of personnel security controls. According to the National Institute of Standards and Technology (NIST), personnel security controls help organizations ensure that individuals occupying positions of responsibility (including third-party service providers) are trustworthy and meet established security criteria for those positions. Organizations should also ensure that information and information systems are protected during and after personnel actions, such as terminations and transfers. More specifically, the *Internal Revenue Manual* requires that all accounts be deactivated within 1 week of an individual's departure on friendly terms and immediately upon an individual's departure on unfriendly terms.

IRS did not always ensure that personnel security controls were fully implemented. For example, at three locations, IRS did not remove application access within 1 week of separation for 6 of 17 (35 percent) separated employees we reviewed. IRS also did not deactivate proximity cards immediately upon employee separation at one of its facilities. As a result, IRS is at an increased risk that individuals could gain unauthorized access to its resources.

IRS Had Not Fully Implemented All Elements of Its Information Security Program

A key reason for the information security weaknesses in IRS's financial and tax processing systems is that it has not yet fully implemented its agencywide information security program to ensure that controls are effectively established and maintained. FISMA requires each agency to develop, document, and implement an information security program that, among other things, includes

- periodic assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems;

- policies and procedures that (1) are based on risk assessments, (2) cost effectively reduce information security risks to an acceptable level, (3) ensure that information security is addressed throughout the life cycle of each system, and (4) ensure compliance with applicable requirements;

- plans for providing adequate information security for networks, facilities, and systems;

- security awareness training to inform personnel of information security risks and of their responsibilities in complying with agency policies and procedures, as well as training personnel with significant security responsibilities for information security;

- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls for every system identified in the agency's required inventory of major information systems;

- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in its information security policies, procedures, or practices; and

- plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

IRS has made important progress in developing and documenting elements of its information security program. However, not all components of its program have been fully implemented.

Although a Risk Assessment Process Was Implemented, Assessments Were Not Always Annually Reviewed

According to NIST, risk is determined by identifying potential threats to the organization and vulnerabilities in its systems, determining the likelihood that a particular threat may exploit vulnerabilities, and assessing the resulting impact on the organization's mission, including the effect on sensitive and critical systems and data. Identifying and assessing information security risks are essential to determining what controls are required. Moreover, by increasing awareness of risks, these assessments can generate support for the policies and controls that are adopted in order to help ensure that these policies and controls operate as intended. Consistent with NIST guidance, IRS requires its risk assessment process to detail the residual risk[9] assessed, as well as potential threats, and to recommend corrective actions for reducing or eliminating the vulnerabilities identified. IRS also requires system risk assessments be reviewed annually.

Although IRS had implemented a risk assessment process, it did not always annually review its risk assessments. The risk assessments that we reviewed were current, documented residual risks assessed, as well as potential threats, and recommended corrective actions for mitigating or eliminating the vulnerabilities that were identified. However, two risk assessments for systems supporting tax processing and inventory control had not been reviewed annually, per IRS's policy. As a result, potential

[9] Residual risk is the risk remaining after the implementation of new or enhanced controls.

risks to these systems and the adequacy of their management, operational, and technical controls to reduce risks may be unknown.

IRS Had Developed and Documented Policies and Procedures for Key Elements of Its Information Security Program

Another key element of an effective information security program is to develop, document, and implement risk-based policies, procedures, and technical standards that govern security over an agency's computing environment. If properly implemented, policies and procedures should help reduce the risk associated with unauthorized access or disruption of services. Technical security standards can provide consistent implementation guidance for each computing environment. Developing, documenting, and implementing security policies are the important primary mechanisms by which management communicates its views and requirements; these policies also serve as the basis for adopting specific procedures and technical controls. In addition, agencies need to take the actions necessary to effectively implement or execute these procedures and controls. Otherwise, agency systems and information will not receive the protection that the security policies and controls should provide.

IRS has developed and documented information security policies, standards, and guidelines that generally provide appropriate guidance to personnel responsible for securing information and information systems. This has included guidance for assessing risk, security planning, security training, testing and evaluating security controls, contingency planning, and guidance for operating system platforms. However, as illustrated by the weaknesses identified in this report, IRS has not yet fully implemented its policies, standards, and guidelines.

Security Plans Adequately Documented Management, Operational, and Technical Controls

An objective of system security planning is to improve the protection of information technology resources. A system security plan provides an overview of the system's security requirements and describes the controls that are in place or planned to meet those requirements. OMB Circular A-130 requires that agencies develop system security plans for major applications and general support systems, and that these plans address policies and procedures for providing management, operational, and technical controls. Furthermore, IRS policy requires that security plans be developed, documented, implemented, and periodically updated for the controls in place or planned for an information system.

IRS had developed, documented, and updated the plans for eight systems we reviewed. Furthermore, those plans documented the management, operational, and technical controls in place and included information required per the OMB Circular A-130 for applications and general support systems. However, as illustrated by weaknesses identified in this report, IRS had not yet fully implemented all the controls documented in its security plans.

Security Awareness and Specialized Training Was Provided for All Employees Reviewed

People are one of the weakest links in attempts to secure systems and networks. Therefore, an important component of an information security program is providing sufficient training so that users understand system security risks and their own role in implementing related policies and controls to mitigate those risks. IRS policy requires that personnel performing information technology security duties meet minimum continuing professional education hours in accordance with their roles. Personnel performing security roles are required by IRS to have 12, 8, or 4 hours of specialized training per year, depending on their specific role.

IRS personnel performing information technology security duties met their minimum continuing professional education requirements. For the employees and contractors with specific security-related roles that we reviewed, 36 employees and contractors at one data center, and 24 employees and contractors at another, met the required minimum security awareness and specialized training hours.

Although Controls Were Tested and Evaluated, Tests Were Not Always Comprehensive

Another key element of an information security program is to test and evaluate policies, procedures, and controls to determine whether they are effective and operating as intended. This type of oversight is a fundamental element because it demonstrates management’s commitment to the security program, reminds employees of their roles and responsibilities, and identifies and mitigates areas of noncompliance and ineffectiveness. Although control tests and evaluations may encourage compliance with security policies, the full benefits are not achieved unless the results improve the security program. FISMA requires that the frequency of tests and evaluations be based on risks and occur no less than annually. IRS policy also requires periodic testing and evaluation of the effectiveness of information security policies and procedures.

Although IRS had a process in place for testing and evaluating its systems, the process was not comprehensive. IRS had tested and evaluated information security controls for each of the eight systems we reviewed. However, its testing process did not identify certain weaknesses that we identified during our review. For example, IRS was not testing for complex passwords on its UNIX servers at one data center. Additionally, from an enterprisewide perspective, the agency had not identified inappropriate access to numerous shares containing sensitive information. Until IRS improves its testing of controls over its systems, it has reduced assurance that its policies and procedures are being followed and that controls for its systems are being effectively implemented and maintained.

Although Remedial Action Plans Were Complete, Corrective Actions Were Not Always Validated

A remedial action plan is a key component described in FISMA. Such a plan assists agencies in identifying, assessing, prioritizing, and monitoring progress in correcting security weaknesses that are found in information systems. In its annual FISMA guidance to agencies, OMB requires agency remedial action plans, also known as plans of action and milestones, to include the resources necessary to correct identified weaknesses. According to IRS policy, the agency should document weaknesses found during security assessments, as well as document only planned, implemented, and evaluated remedial actions to correct any deficiencies. The policy further requires that IRS track the status of resolution of all weaknesses and verify that each weakness is corrected.

Although remedial action plans were in place, corrective actions were not always appropriately validated. IRS has developed and implemented a remedial action process to address deficiencies in its information security policies, procedures, and practices. However, this remedial action process was not working as intended, since the verification process used to determine whether remedial actions were implemented was not always effective. For example, IRS had informed us that it had completed actions to close 65 recommendations related to previously identified weaknesses, however, we determined that 16 of the corrective actions did not mitigate or correct the underlying control deficiencies. Without a sound remediation process, IRS will not have assurance that it has taken the necessary actions to correct weaknesses in its policies, procedures, and practices. We have previously identified a similar weakness and recommended that IRS implement a revised remedial action verification process that ensures actions are fully implemented, but the condition continued to exist at the time of our review.

Although Contingency Plans Were Annually Reviewed and Tested, IRS Recognizes the Need for Further Efforts

Continuity of operations planning, which includes contingency planning and disaster recovery planning, is a critical component of information protection. To ensure that mission-critical operations continue, it is necessary to be able to detect, mitigate, and recover from service disruptions while preserving access to vital information. It is important that these plans be clearly documented, communicated to potentially affected staff, and updated to reflect current operations. In addition, testing contingency plans is essential to determine whether the plans will function as intended in an emergency situation. FISMA requires that agencywide information security programs include plans and procedures to ensure continuity of operations. IRS contingency planning policy requires, among other things, that contingency plans be reviewed and tested at least annually.

Although contingency plans were in place, IRS recognizes the need for improvements. The agency has completed contingency plans for the eight systems we reviewed. Additionally, it has reviewed/updated and tested these contingency plans annually.[10] The plans also identified critical business processes, correcting a weakness we reported last year. Although the specific plans we reviewed did not have any shortcomings, IRS's comprehensive plan for addressing information security weaknesses recognizes the need for further efforts to improve the agency's contingency planning, through initiatives involving disaster recovery planning, some of which will not be completed until 2011. Until it completes these efforts, IRS is at increased risk of not being able to effectively recover and continue operations when an emergency occurs.

Conclusions

IRS has made progress in correcting or mitigating previously reported weaknesses, implementing controls over key financial systems, and developing and documenting a framework for its agencywide information security program. Information security weaknesses—both old and new—continue to impair the agency's ability to ensure the confidentiality, integrity, and availability of financial and taxpayer information. These deficiencies represent a material weakness in IRS's internal controls over its financial and tax processing systems. A key reason for these weaknesses is that the agency has not yet fully implemented certain key elements of its agencywide information security program. The financial and taxpayer information on IRS systems will remain particularly vulnerable to insider threats until the agency (1) begins to address and correct prior weaknesses across the service and (2) fully implements a comprehensive agencywide information security program that ensures risk assessments are appropriately reviewed for all systems, tests and evaluations of controls for systems are comprehensive, and the remedial action process effectively validates corrective actions. Until IRS takes these steps, financial and taxpayer information are at increased risk of unauthorized disclosure, modification, or destruction, and the agency's management decisions may be based on unreliable or inaccurate financial information.

[10] We did not test the effectiveness of IRS's contingency plan testing.

Recommendations for Executive Action

In addition to implementing our previous recommendations, we recommend that you take the following two actions to implement an agencywide information security program:

- ensure risk assessments for IRS systems are reviewed at least annually, and
- implement steps to improve the scope of testing and evaluating controls, such as those for weak passwords.

We are also making eight detailed recommendations in a separate report with limited distribution. These recommendations consist of actions to be taken to correct specific information security weaknesses related to authorization, physical security, and configuration management identified during this audit.

Agency Comments

In providing written comments (reprinted in app. II) on a draft of this report, the Commissioner of Internal Revenue stated that the security and privacy of taxpayer information is of the utmost importance to the agency, and noted that IRS is committed to securing its computer environment as it continually evaluates processes, promotes user awareness and applies innovative ideas to increase compliance. He also stated that the agency is working to improve its security posture, and will develop a detailed corrective action plan addressing each of our recommendations.

This report contains recommendations to you. As you know, 31 U.S.C. 720 requires the head of a federal agency to submit a written statement of the actions taken on our recommendations to the Senate Committee on Homeland Security and Governmental Affairs and to the House Committee on Oversight and Government Reform not later than 60 days from the date of the report and to the House and Senate Committees on Appropriations with the agency’s first request for appropriations made more than 60 days after the date of this report. Because agency personnel serve as the primary source of information on the status of recommendations, GAO requests that the agency also provide us with a copy of your agency’s statement of action to serve as preliminary information on the status of open recommendations.

We are sending copies of this report to interested congressional committees, the Secretary of the Treasury, and the Treasury Inspector General for Tax Administration. The report also is available at no charge on the GAO Web site at http://www.gao.gov.

If you have any questions regarding this report, please contact Nancy Kingsbury at (202) 512-2700 or Gregory C. Wilshusen at (202) 512-6244. We can also be reached by e-mail at kingsburyn@gao.gov and wilshuseng@gao.gov. Key contributors to this report are listed in appendix III.

Sincerely yours,

Nancy R. Kingsbury

Nancy R. Kingsbury,
Managing Director, Applied Research and Methods

Gregory C. Wilshusen

Gregory C. Wilshusen
Director, Information Security Issues

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to determine (1) the status of the Internal Revenue Service's (IRS) actions to correct or mitigate previously reported information security weaknesses and (2) whether controls over key financial and tax processing systems were effective in protecting the confidentiality, integrity, and availability of financial and sensitive taxpayer information. This work is part of our audit of IRS's financial statements for the purpose of supporting our opinion on internal controls over the preparation of those statements.

To determine the status of IRS's actions to correct or mitigate previously reported information security weaknesses, we reviewed prior GAO reports to identify previously reported weaknesses and examined IRS's corrective action plans to determine which weaknesses IRS reported corrective actions as being completed. For those instances where IRS reported it had completed corrective actions, we assessed the effectiveness of those actions by:

- testing the complexity and expiration of passwords on servers to determine if strong password management was enforced;
- analyzing users' system authorizations to determine whether they had more permissions than necessary to perform their assigned functions;
- observing data transmissions across the network to determine whether sensitive data was being encrypted;
- observing whether system security software was logging successful system changes;
- testing and observing physical access controls to determine if computer facilities and resources were being protected from espionage, sabotage, damage, and theft;
- inspecting key servers and workstations to determine whether critical patches had been installed or were up-to-date; and
- examining access responsibilities to determine whether incompatible functions were segregated among different individuals.

We evaluated IRS's implementation of these corrective actions for three data centers and an additional facility.

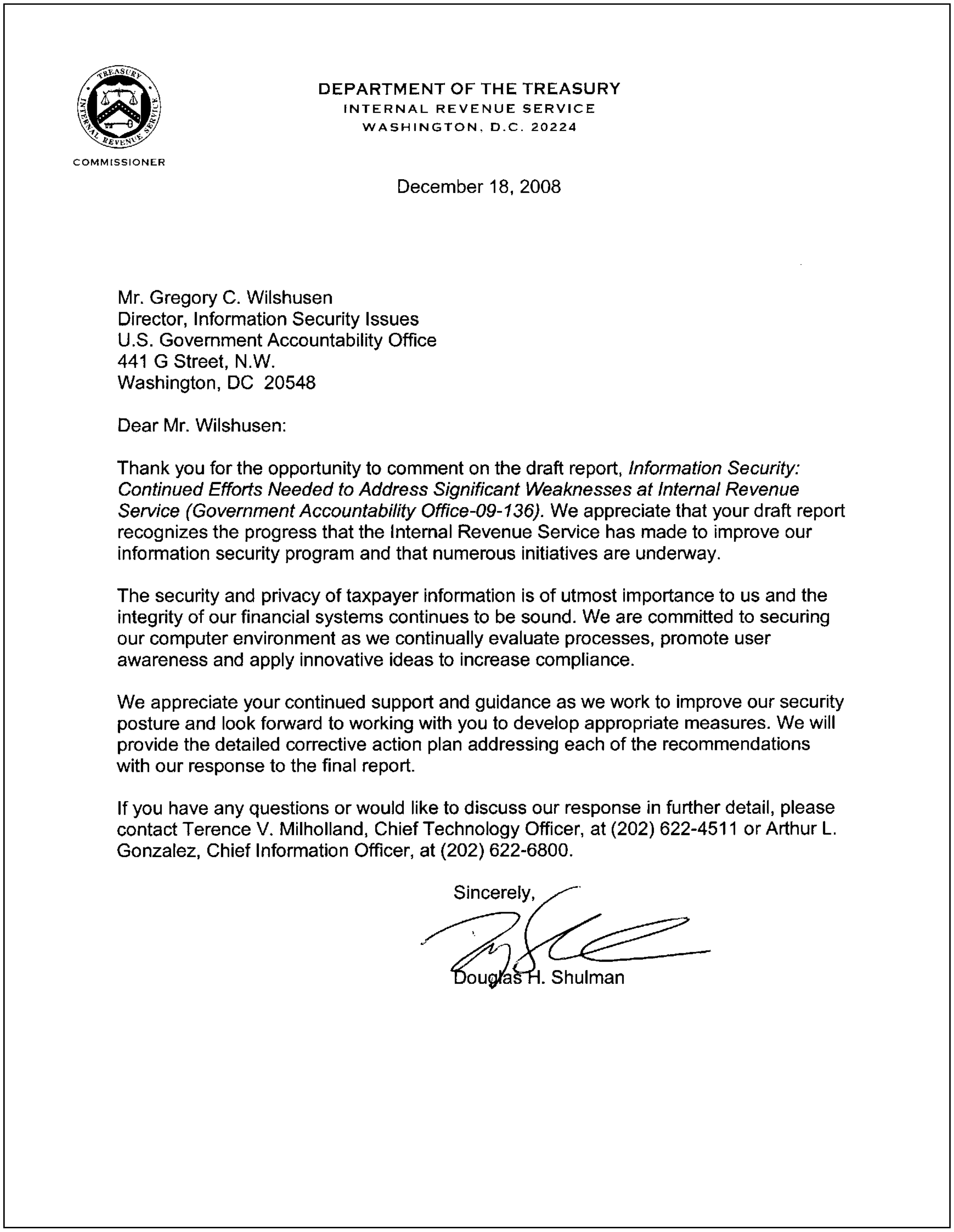
To determine whether controls over key financial and tax processing systems were effective, we considered the results of our evaluation of IRS's actions to mitigate previously reported weaknesses at three data centers and the additional facility. We concentrated our evaluation primarily on threats emanating from sources internal to IRS's computer networks and focused on three critical applications and their general support systems that directly or indirectly support the processing of material transactions that are reflected in the agency's financial statements. Our evaluation was based on our *Federal Information System Controls Audit Manual*, which contains guidance for reviewing information system controls that affect the confidentiality, integrity, and availability of computerized information.

Using the requirements identified by the Federal Information Security Management Act, which establishes key elements for an effective agencywide information security program, we evaluated IRS's implementation of its security program by

- analyzing IRS's risk assessment process and risk assessments for eight key IRS financial and tax processing systems to determine whether risks and threats were documented;
- analyzing IRS's policies, procedures, practices, and standards to determine whether sufficient guidance was provided to personnel responsible for securing information and information systems;
- analyzing security plans for eight systems to determine if management, operational, and technical controls were documented and if security plans were updated;
- examining training records for personnel with significant responsibilities to determine if they received training commensurate with those responsibilities;
- analyzing test plans and test results for eight IRS systems to determine whether management, operational, and technical controls were tested at least annually and based on risk;
- observing IRS's process to correct weaknesses and determining whether remedial action plans were complete; and
- examining contingency plans for eight IRS systems to determine whether those plans had been tested or updated.

We also reviewed or analyzed previous reports from the Treasury Inspector General for Tax Administration and GAO; and discussed with key security representatives and management officials whether information security controls were in place, adequately designed, and operating effectively.

Appendix II: Comments from the Internal Revenue Service



DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

COMMISSIONER

December 18, 2008

Mr. Gregory C. Wilshusen
Director, Information Security Issues
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Mr. Wilshusen:

Thank you for the opportunity to comment on the draft report, *Information Security: Continued Efforts Needed to Address Significant Weaknesses at Internal Revenue Service (Government Accountability Office-09-136).* We appreciate that your draft report recognizes the progress that the Internal Revenue Service has made to improve our information security program and that numerous initiatives are underway.

The security and privacy of taxpayer information is of utmost importance to us and the integrity of our financial systems continues to be sound. We are committed to securing our computer environment as we continually evaluate processes, promote user awareness and apply innovative ideas to increase compliance.

We appreciate your continued support and guidance as we work to improve our security posture and look forward to working with you to develop appropriate measures. We will provide the detailed corrective action plan addressing each of the recommendations with our response to the final report.

If you have any questions or would like to discuss our response in further detail, please contact Terence V. Milholland, Chief Technology Officer, at (202) 622-4511 or Arthur L. Gonzalez, Chief Information Officer, at (202) 622-6800.

Sincerely,

Douglas H. Shulman

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Nancy R. Kingsbury, (202) 512-2700, kingsburyn@gao.gov

Gregory C. Wilshusen, (202) 512-6244, wilshuseng@gao.gov

Staff Acknowledgments

In addition to the individuals named above, David Hayes (Assistant Director), Jeffrey Knott (Assistant Director), Harold Lewis (Assistant Director), Larry Crosland, Mark Canter, Sharhonda Deloach, Neil Doherty, Caryn English, Edward Glagola, Nancy Glover, Rebecca LaPaze, Kevin Metcalfe, Zsaroq Powe, Eugene Stevens, and Christy Tyson made key contributions to this report.

(311017)

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548